BY ORDER OF THE COMMANDER
AIR FORCE MATERIEL COMMAND

AIR FORCE INSTRUCTION 33-211

AIR FORCE MATERIEL COMMAND
Supplement 1

11 OCTOBER 2002

Communications and Information

COMMUNICATIONS SECURITY (COMSEC) USER REQUIREMENTS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AFMC WWW site at: https://www.afmc-mil.wpafb.af.mil/pdl/

OPR: AFMC CSO/SCON
(Mr. Harry A. Wildermuth)
Supersedes AFI 33-211/AFMCS1, 12 Jan 96

Certified by: AFMC CSO/SCO
(Lt. Col Kenneth A. Jeter)
Pages: 8
Distribution: F

This supplement establishes command-unique Communications Security (COMSEC) management requirements. It defines policies and procedures applicable to COMSEC Managers (CMs), COMSEC Responsible Officers (CROs), COMSEC User Agencies (UAs), and contractors receiving COMSEC support from or managing AFMC-gained COMSEC accounts. Each CM is responsible for developing a supplement outlining local procedures for the CROs and UAs. Base supplements can add to, but not take away from the Air Force Instruction (AFI) and major command supplement. This supplement applies to all users who receive COMSEC material from AFMC COMSEC accounts, to include US Air Force Reserve (AFR) units. This publication only applies to the Air National Guard (ANG) units when published in the ANGIND 2.

SUMMARY OF REVISIONS

Clarifies and updates guidance for AFMC COMSEC users.

AFI33-211, 1 November 1997, is supplemented as follows:

3. The Facility Security Officer (FSO) or equivalent will be the authorizing official for Air Force contractor COMSEC UAs and activities. The CRO and alternates must have a final security clearance and access. Do not use the COMSEC access list as the CRO and alternate CRO appointment letter. Maintain a copy of the CRO and alternate CRO appointment letter with the UAs COMSEC records.

3.1. Forward all waivers concerning appointments for CROs and alternate CROs to the CM. Although the CM generally does not approve or disapprove waivers, the CM must review all waivers and advise the appointing commander whenever the one-grade limit is exceeded, or the appointee lacks sufficient experience or responsible approach regarding COMSEC-related matters. Reducing minimum grades by more than one level, i.e., E-3 vice E-5 for primary CRO, requires approval from headquarters. Forward such requests through the CM to HQ AFMC COMSEC office (AFMC CSO/SCON).

3.2. Contact the CM upon notification of pending transfers.

4.1.2. Maintains a copy of the COMSEC requirements with the UAs COMSEC records.

4.1.6. (Or a designated individual assigned to the main account), conducts initial and annual training for each CRO and Alternate CRO appointed using the AF Form 4168, **COMSEC Responsible Officer and User Training Checklist**.

4.1.7. (Added) Prior to providing any service to a contractor COMSEC UA or activity, obtains a copy of the DD Form 254, DoD Contract Security Classification Specification, to determine authorization to COMSEC material, classification levels, and authority to use and store this material.

4.2.6. (Added) Ensures transfer of accountability for all COMSEC material to a new CRO prior to the CRO being relieved of COMSEC responsibilities (i.e., change of duty assignment, permanent change of station, retirement, etc.). If deemed appropriate, ensures CROs who will be deploying on temporary duty (TDY) for periods greater than 90 days report to the CM to be relieved of accountability for COMSEC materials they have signed for, in order for another CRO to sign and receipt for material from the COMSEC account.

4.3.1. Contact the CM upon notification of pending requirements.

4.3.2. Include COMSEC equipment items and associated publications issued on SF Form 153s on the requirements letter.

4.3.3. If a contractor, will refer to appropriate company-produced rosters.

4.3.4. If a contractor, may use appropriate company-produced forms if AF Forms 1109**, Visitor Register Logs**, are not available. The current month's company produced form, plus the previous 3 months must be kept on file.

4.3.5. Ensure personnel remain proficient on all checklist items contained in AF Form 4168 when conducting annual refresher training. While it is not necessary to conduct in-depth training on each item, the supervisor or trainer must review all items that apply to the work center with each individual.

4.3.5.1. (Added) Ensure all users complete refresher training not more than 30 days following the anniversary of the last formal COMSEC training (initial or refresher). Remove and destroy all training documentation on individuals when they no longer require access to COMSEC material.

4.3.7. Contracting personnel must prepare and use company Standard Practice Procedures (SPP) in place of operating instructions.

4.3.9. Ensure the following ALC inventory requirements are complied with: ALC-6 (electronic material) is inventoried the same as ALC-1 material. ALC-7 electronic material is treated the same as ALC-4 material. Contact the CM for assistance concerning specific inventory requirements. Also, see AFI 33-211, paragraph 11.

4.3.14. Will refer to attachment 7 of this supplement for specific records disposition instructions.

4.3.18. Ensure the CM provides instructions for non-duty hour notification.

4.3.19. Validate semiannual training compliance. All personnel must sign and date review documentation developed by the CRO. Personnel on leave or TDY must complete and document the training upon return.

4.3.20. Remove users when they no longer meet the requirements for enrollment according to AFI 33-210, *Cryptographic Access Program*.

5. Notify the CM on all matters concerning removal and/or reproduction of COMSEC materials. DO NOT reproduce cryptographic keying materials without prior approval from the appropriate COMSEC controlling authority. Obtain any such approval through COMSEC channels. Violations of this paragraph can result in severe administrative disciplinary, and/or judicial actions.

6.2. Contractors not supported by the Standard Base Supply System will process COMSEC equipment requests through the COMSEC Material Control System.

7. A final security clearance is required by all personnel who have access to COMSEC material.

8.3. The CRO ensures aircrews receiving COMSEC material in support of flying missions are adequately briefed on COMSEC handling responsibilities. Develop training pertinent to the flying mission being supported. Add, as a minimum, general responsibilities to the Standard Form 153, **COMSEC Material Report**, or local hand receipt used, to issue COMSEC material. If aircrew members are responsible for authenticating and/or decoding nuclear control orders (valid or exercise), they must be formally enrolled in the cryptographic access program IAW AFI 33-210, Para 1.6. Outline these procedures in local operating instructions.

9. Contractors will contact the Air Force representative at their location to order forms and publications or gain access to the necessary Air Force web sites in order to download the necessary forms and publications. If an Air Force representative is not available, contact AFMC CSO/SCON to obtain forms and publications.

10.2. Refer to attachment 2 of this supplement for specific records disposition instructions.

10.2.1. Only the CM's staff, higher headquarters' COMSEC staff members, and nuclear surety inspection (NSI) team members during an NSI are authorized access to COMSEC and COMSEC users' records. Do not allow access to other inspection, periodic review, and staff assistance personnel without prior approval from AFMC CSO/SCON.

10.4. (Added) The CM defines how COMSEC records maintained by the CRO will be organized. As a minimum, records will include the following: OIs, emergency action plans (EAP), appointment letters, access and requirements lists, AFCOMSEC Form 9, **Cryptographic Access Certificate**, AF Forms 1109, AF Forms 4168, COMSEC inventories, destruction reports, hand receipts, and waivers.

11.1.1. Inventory keytape canisters according to paragraph 19.4 (basic document).

14.3. Contractors will refer to appropriate company-produced rosters. Review company-produced documents monthly to ensure its accuracy and then mark review date and their initials on the list once clearances are verified.

14.5. Contractors may use appropriate company-produced forms if AF Forms 1109 are not available.

16. Unapproved containers are not authorized for stand-alone protection of classified material. However, the use of non-GSA approved safes and security containers as locking file cabinets within approved vaults or continuously manned areas is authorized.

16.2.2. Store and protect Data Transfer Devices (DTDs) according to the highest classification of the key and data contained therein, when the DTD Cryptographic Ignition Key (CIK) is inserted. If the CIK is separated from the DTD and locked in an approved security container, protect the DTD as unclassified

ALC-1 and inventory accordingly. If the DTD doesn't contain any classified key or data, store and protect it as a controlled cryptographic item, ALC-1 on the AFCOMSEC Form 16.

16.4.4.1. Certified locksmiths should inspect the integrity of safes containing COMSEC material at least once every 5 years (your unit security manager may require this to take place every 2 years). This inspection should be documented on the Air Force Technical Order (AFTO) Form 36, **Maintenance Record for Security Type Equipment** maintained in the safe. Safe combination changes do not need to be recorded on the AFTO Form 36.

16.5. Change a cipher lock combination when personnel knowing the combination no longer require access to the facility, their access to the facility is suspended/revoked, or at least monthly.

17.5.5. (Added) COMSEC equipment using removable CIKs has the CIKs properly secured, appropriate to the work center's storage requirements. This includes equipment such as, but not limited to KG-95, KG-194, Network Encryption Standard equipment, Secure Data Network System equipment, and STU-III telephones.

17.6. Contractors may use appropriate company-produced forms if standard forms, Air Force forms, and Department of Defense forms aren't available.

18. Review and update OIs when significant changes occur. In addition to subject areas required in paragraph 18 (basic document), ensure keytape verification and disposition procedures, as they pertain to inventory and accounting requirements, are also included in all UA OIs.

18.1. (Added) Civilian defense contractors will use company SPPs in place of operating instructions. Companies contracted to operate base communications services, including COMSEC accounts, will use operating instructions.

19.2.1. When correcting inventory discrepancies and making explanatory remarks on the reverse side of the inventory, include the date the discrepancy was discovered and corrected, a detailed description of the discrepancy, and the initials of the individual who made the correction.

19.4. When all items have been properly accounted for, place an “X” in the appropriate block on the AFCOMSEC Form 16, **COMSEC Account Daily Shift Inventory**, AFCOMSEC Form 23, **COMSEC Account Local Inventory Report**, or company-produced forms for contractor accounts.

19.6. Keep completed keytape canister disposition records with the spent canisters until you have opened and inspected those canisters for any remaining keytape residue. Once the canisters have been inspected, prepare and complete a local destruction report and dispose of disposition records as directed by the CM.

19.8. To simplify COMSEC material audits, when using CM2 the COMSEC account and UAs will only print new inventories when adding, transferring, or removing material if there are 12 or more line items added or removed. On the new inventories, identify all added material. On old inventories, identify material removed and their disposition (i.e., issued to UA number 1, removed for destruction, moved to safe #3, etc.).

19.10. Stamp the highest classification and handling caveat (i.e., NOFORN) of the sealed package contents on the outside of the package. Use paper tape, with fiber reinforcement, to seal packages.

19.13. Document these reviews by placing an entry on the first page of the inventory (for each safe) containing the date the review was conducted and the initials of the person doing the review. Provide follow-up training on inventory procedures to individuals as needed.

24. The CRO will immediately advise the CM when destruction facilities are not available for routine destruction of COMSEC material. Solicit alternative destruction options to destroy COMSEC material within prescribed time limits.

25.2. Document any extension, except weekends and holidays, granted beyond the 12-hour limit after supersession. Include justification for extension (i.e., needed to rekey an unstable circuit), names of individuals granting the extension, dates, times, etc. Maintain record of extension for the period the keying material is effective. Record may be destroyed upon whole supersession of keying material.

27.1. The destruction official will be listed on the UAs COMSEC access list.

27.3. Destruction and witnessing officials must closely observe the actual destruction and ensure all destruction documentation is complete and accurate. They must thoroughly search destruction residue to ensure complete destruction.

34.1. Use an official memorandum to document names and the specific lock to which each individual is granted access.

40.1. The CM must sign and date the last card for each plan (i.e., fire, bomb threat, and natural disaster). All revisions must be coordinated with the CM before implementation. There is no requirement to publish an EAP for users holding only ALC-4 material.

41.1. FSOs should coordinate on EAPs prepared by the contractor facility CRO. The contractor COMSEC manager provides assistance as needed.

41.3.2. Document initial EAP instruction/training. Include trainees' names, dates trained, and EAPs covered. Trainees must sign or initial documentation.

41.3.3. Document all EAP reviews, dry-runs, and actual events. For dry-runs and actual events, include the EAP used, date, location, persons participating, and a brief description of circumstances and results. Each participant must, as a minimum, initial and date any documentation pertaining to reviews, dry-runs, and actual events. Records of actual events may be used to fulfill semiannual review and dry-run requirements.

41.3.3.1. (Added) Ensure individuals not available to participate in EAP training exercises (i.e., TDY, leave, etc.) are rescheduled for training immediately upon return. Maintain all EAP training documentation from one command functional review to the next.

42.9. Coordinate the emergency plan at least every 3 years, or when significant changes occur.

43. If using the sample task cards in attachment 5 from the basic document, make sure that all required information from paragraphs 42 and 43 in the basic document are included. The sample task cards listed in attachment 5 may not list all required entries/actions to support all duty sections.

43.1. Ensure names of all emergency personnel (fire, bomb, medical, etc.) are obtained and recorded for the purpose of presenting these individuals with inadvertent exposure oaths, if necessary.

53.4. The inquiry or investigating official must provide a copy of the completed report to the CM for additional comments and submission through COMSEC channels to higher headquarters.

58.3. Replies must address the specific actions to correct and eliminate the basic cause of the deficiencies and provide enough detail to permit effective evaluation.

Attachment 1

GLOSSARY OF ABBREVIATIONS AND ACRONYMS

Abbreviations and Acronyms

CIK-Cryptographic Ignition Key

CM-COMSEC Manager

CRO- COMSEC Responsible Officer

DoD-Department of Defense

DTD-Data Transfer Device

EAP- Emergency Action Plan

FSO-Facility Security Officer

NSI-Nuclear Surety Inspection

SPP-Standard Practice Procedure

DTD-Data Transfer Device

EAP-Emergency Action Plan

FSO-Facility Security Officer

NSI-Nuclear Surety Inspection

SPP-Standard Practice Procedure

Attachment 7

COMSEC RECORDS DISPOSITION INSTRUCTIONS

Use the following guide for maintain and disposing of COMSEC records:

Form/Document	Instructions
AFCOMSEC Form 1, **COMSEC Users Receipt/ Destruction Certificate**	Destroy when local destruction report is accomplished.
AFCOMSEC Form 21, **Disposition Record for KI-1B/C Keytapes**	Destroy when local destruction report is accomplished.
AFCOMSEC Form 22A, **Disposition Record for Single Copy Keytapes**	Destroy when local destruction report is accomplished.
AFCOMSEC Form 22B, **Disposition Record for Multi-copy Keytapes**	Destroy when local destruction report is accomplished.
AFCOMSEC Form 9**, Cryptographic Access Certificate**	Destroy 90 days after date of withdrawal, unless withdrawn for cause. In that case, destroy when all inquiries/investigations are completed.
AFCOMSEC Form 16, **COMSEC Account Daily Shift Inventory**	Maintain current plus 6 months.
AF Form 4168, **COMSEC Responsible Officer and User Training Checklist**	Maintain all training documentation from one command COMSEC functional review to the next.
AF Form 1109, **Visitor Register Log**	Maintain current plus 3 months.
AFTO Form 36, **Maintenance Record for Security Type Equipment**	Permanent. Keep with safe.
SF 700, **Security Container Information**	Destroy when superceded.
SF 701, **Activity Security Checklist**	Maintain current only.
SF 702, **Security Container Check Sheet**	Maintain current only.
Local Destruction Reports Hand Receipts (SF 153, **COMSEC Material Report**)	Destroy 2 years after date of material destruction.
All Waivers	Maintain original and all renewals until the waiver is terminated.
Form/Document	Instructions
Operating Instructions (with coordination)	Maintain current only.
EAPs (with coordination)	Maintain current only.
EAP Dry Run Records	Destroy after next command COMSEC functional review.
Functional Review Reports and Follow-ups (MAJCOM and wing)	Destroy after next command COMSEC functional review.
COMSEC Incident Reports and Follow-ups	Destroy 1 year after date report is closed.
Facility Access Lists	Maintain current only.

Form/Document	Instructions
Functional Review, Visitor, and COMSEC Manager Access Lists	Maintain current only.
Technical Countermeasures Surveys	Maintain current only.
Two-Person Integrity Appointments	Maintain current only.
Primary and Alternate CRO Appointments	Maintain current only.
Courier Letters	Maintain current only.
Hand Receipts (SF 153)	Destroy when all material listed on any given hand receipt is destroyed or transferred.

KENNETH I. PERCELL, Director
Information Technology